SKYBOX SECURITY

Reduce compliance and vulnerability risks in the public sector

Manage your attack surface, adopt a Zero Trust approach, and comply with BOD 22-01 with the Skybox Security Posture Management Platform

Challenges

In our modern digital world, risk comes in many forms. All organizations must contend with the expanding cybersecurity threats and business risks of a dynamic and complex attack surface. Prolific threat actors, such as the Lapsus$ cybercriminal collective, are creating devastating damage with modest resources. The recent ransomware attack orchestrated by this group against the Brazilian Ministry of Health, for example, compromised critical information systems that support Brazil's national immunization program and digital vaccination certificates. This caused delays to the administration's plan for implementing new health requirements for arriving travelers. This reminder that cybercrime spares no country or organization hits particularly close to home for organizations in the U.S. public sector that face unique challenges in defending against cyber risk.

Risk factors

- **Difficulty meeting regulatory requirements in fragmented environments**
- **Limited visibility across the entire attack surface**
- **Risk of non-compliance without holistic view of hybrid infrastructure**
- **Inconsistent security policies increase breach risk**
- **Increased vulnerabilities due to hidden exposures**
- **Siloed and disparate teams, systems, and technologies**
- **Shortage of specialized resources for cyber management**

The most new vulnerabilities published in a single year.

20,175

10% increase from 2020 to 2021 – biggest YoY growth[1]

[1] Vulnerability and Threat Trends Report 2022, Skybox, April 2022

Challenges

Lack of visibility and context across on-premise, hybrid, and multi-cloud environments make it especially difficult to navigate two aspects of risk management. The first is compliance. The surge of new compliance frameworks, evolving regulatory requirements, and internal security policies add pressure to IT and security teams who struggle to keep up. The challenges are compounded for public sector organizations with multiple locations, hybrid environments, and numerous cybersecurity point products. The recent memorandum on Zero Trust Cybersecurity Principles requires agencies to meet specific Zero Trust standards and objectives by the end of fiscal year 2024.[2] This sweeping, administration-wide effort to modernize cybersecurity approaches has many organizations unsure of where to begin.

The second aspect is vulnerability management. The restricted view in a siloed environment impacts an organization's ability to identify and address exposures and adhere to Security Technical Implementation Guide (STIG) configuration standards. The Binding Operational Directive BOD-22-01 issued by the U.S. Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA) drives an urgent call-to-action to federal civilian agencies.[3] Under this directive, these organizations are now mandated to quickly remediate a prioritized list of known and exploited vulnerabilities.[4] For many, adherence to these mandates while meeting the associated aggressive timelines represents a complex undertaking, especially due to the growing cybersecurity talent gap.

34%

of public sector organizations said they are not well prepared for a rapidly changing threat landscape[5]

37%

of public sector organizations said "inadequate identification of key risks" poses the biggest cybersecurity challenge[6]

Ultimately, the fragmented and decentralized nature of their environments places public sector organizations at varying levels of risk. To comply with current and future directives, adhere to STIG standards, and effectively defend against threats, U.S. federal agencies must gain a full understanding of their attack surface.

[2] Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, Office of Management and Budget, January 26, 2022
[3] Binding Operational Directive 22-01 Reducing the Significant Risk of Known Exploited Vulnerabilities, CISA, November 3, 2021
[4] Known Exploited Vulnerabilities Catalog, CISA, November 3, 2021
[5,6] Cybersecurity solutions for a riskier world, Thoughtlab, May 2022

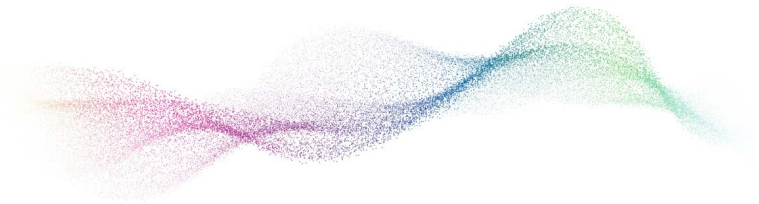
Solution

Compliance risks

It is a well-known cybersecurity maxim that it is impossible to address the threats that one cannot see. To proactively address breach and compliance risk, Skybox develops a network model – a dynamic representation of an organization's routing tables and configurations across the hybrid infrastructure. This abstraction of the corporate infrastructure allows network and security teams the ability to visualize and understand attack paths, validate network segmentation, and optimize rule sets through simulation tasks executed against the network model.

The Skybox Security Posture Management Platform encodes the standards and requirements for external regulatory frameworks and internal corporate security policies into easily customizable, out-of-the-box templates. The platform allows actual configurations and rules to be validated against policy templates so that violating rules can be pinpointed and rectified quickly. Firewall rule sets can be optimized to eliminate overly permissive rules and reduce the organizational attack surface. This facilitates network policy and firewall audits, helping overworked federal agency staff meet compliance obligations around perimeter visibility, network access and segmentation, configuration hygiene, and vulnerability management. In addition, Skybox automates operational workflows to implement the necessary security controls rapidly and accurately across the environment.

This visual and interactive representation of the organization's entire attack surface combined with context-aware change management can become the cornerstone of a zero-trust strategy. This allows the agency to comply with specific objectives for device visibility and enterprise-wide network isolation as outlined in the earlier-referenced January 26, 2022 memorandum.[7]



Vulnerability risks

Demonstrating compliance with BOD 22-01 can become a taxing operational burden for federal agencies. The 655 unique CVEs on the list at the time of this writing could represent millions of vulnerability occurrences across an agency's complex IT estate. The Skybox risk scoring methodology incorporates factors such as asset importance as well as asset and vulnerability exposure which is determined by conducting attack simulation. This helps federal agency staff prioritize remediation efforts by focusing on the vulnerability occurrences that could be most harmful. The Skybox Security Posture Management Platform recommends network-based compensating controls – such as IPS signatures or firewall rule modification – to reduce the risk of imminent attacks. This buys overwhelmed security teams valuable time to plan and deploy patches or update software.

[7] Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, Office of Management and Budget, January 26, 2022

Why Skybox?

Manage your attack surface

Skybox is the only platform that combines infrastructure context with threat intelligence to provide unprecedented visibility of the continuously evolving attack surface. Our network model abstracts the agency's infrastructure, so that small teams can effectively manage complex and heterogeneous IT, OT, and hybrid cloud estates. Actionable insights from our own in-house threat research teams de-risk security policy management.

Adopt a Zero Trust approach

Attack surface modeling and analytics combined with context and risk-aware change automation capabilities from Skybox help agencies rearchitect their infrastructure based on the principles of least-privileged access. Easily customizable, out-of-the-box templates can ensure continuous compliance with zero trust mandates and objectives, avoiding costly audit preparation fees or future non-compliance penalties.

Comply with BOD 22-01

The flexible, customizable Skybox risk scoring methodology ensures a risk posture tailored to an organization's unique environment and operating logic. At the same time, it helps them execute flawlessly within the scope of BOD 22-01. Network-based compensating controls drive a defense-in-depth approach to risk mitigation, allowing for meticulous planning and testing before patch deployment or software update.

Outcomes

+ **Easy compliance with federal directives and mandates**
+ **OpEx savings by avoiding non-compliance penalties, audit preparation fees**
+ **Visibility and context across the expanding attack surface**
+ **Risk reduction through prioritized vulnerability remediation**
+ **Network-based compensating controls allow time for patch deployment**

Want to learn more? Get a demo or talk to an expert:

skyboxsecurity.com/request-demo

ABOUT SKYBOX SECURITY

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. Our Security Posture Management Platform delivers complete visibility, analytics, and automation to quickly map, prioritize, and remediate vulnerabilities across your organization.